# LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

CONF-900706--38

LA-UR--90-2404

DE90 014910

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36



TITLE COMPUTER SECURITY IN DOE DISTRIBUTED COMPUTING SYSTEMS

AUTHOR(S). William J. Hunteman

SUBMITTED TO 31st Annual Meeting of the Institute of Nuclear Materials Management, Los Angeles, July 15-18, 1990

## DISCLAIMER



Los Alamos National Laboratory
Los Alamos, New Mexico 87545

# COMPUTER SECURITY IN DOE DISTRIBUTED COMPUTING SYSTEMS*

W. J. Hunteman
Safeguard Systems Group
Los Alamos National Laboratory
Los Alamos, NM

## ABSTRACT

The modernization of DOE facilities amid limited funding is creating pressure on DOE facilities to find innovative approaches to their daily activities. Distributed computing systems are becoming cost-effective solutions to improved productivity. This paper defines and describes typical distributed computing systems in the DOE. The special computer security problems present in distributed computing systems are identified and compared with traditional computer systems. The existing DOE computer security policy supports only basic networks and traditional computer systems and does not address distributed computing systems. A review of the existing policy requirements is followed by an analysis of the policy as it applies to distributed computing systems. Suggested changes in the DOE computer security policy are identified and discussed. The long lead time in updating DOE policy will require guidelines for applying the existing policy to distributed systems. Some possible interim approaches are identified and discussed.

## 1. INTRODUCTION

The modernization of DOE facilities amid limited funding is pressuring DOE facilities to find innovative approaches to their daily activities. Computing networks and distributed computing systems have become cost-effective solutions to improved productivity. This paper defines and briefly describes typical distributed computing systems in the DOE. The existing DOE computer security policy does not address distributed computing systems. The DOE policy must be updated to accommodate the change in DOE computing environments. The long lead time to update the policy will require the use of innovative interim solutions. Some possible approaches to securing distributed systems are identified and discussed.

*Work supported by the U.S. Department of Energy, Office of Safeguards and Security.

## 2. PROBLEM

The explosion of computer technology and the proliferation of computer-based devices have combined to offer increased cost savings and improved productivity. The available technology includes the entire spectrum of computing systems, from the traditional centralized time-sharing systems to distributed systems.

The distributed systems range from extended computer networks to true distributed systems. The extended networks incorporate a wide variety of computer-based equipment in addition to centralized systems. The true distributed systems integrate, in a transparent manner, the entire spectrum of computer systems and computer-based devices. Virtually every DOE facility is using some form of distributed system. Most are building and using extended networks, but the true distributed systems are beginning to appear.

Information processing at many DOE facilities, especially in handling nuclear materials, requires the use of computer-based devices. These devices are used to control instruments or other activities and to perform limited data processing before the information is delivered to centralized systems. Typically, the information processed by a computer-based device is unclassified until it is integrated with other information (e.g., computation of an inventory difference). However, connection to another computer processing classified information requires the device to conform to the DOE computer security policy for classified systems.

The DOE computer security policy covers all microprocessors, personal computers, controllers, and other stand-alone or special systems that process, store, transfer, or provide access to classified information. The policy views all computer systems, regardless of functionality, as regular computer systems subject to the entire range of threats and policy requirements. The computer security policy is based on a fundamental view that information processing occurs on a single or centralized computing system. The policy does not address the issues of limited functionality (e.g., computer-based instrument controllers) or the broader issue of distributed systems.

## 3. COMPUTER SYSTEMS

The term 'distributed system' has been used for such a wide range of computer networks, multicomputer systems, and multiprocessor systems that it is

difficult to obtain a clear definition. However, for this discussion, we will define distributed systems as loosely-coupled or network based systems.[1]

### 3.1. Traditional Computer Systems

The traditional view of computing systems has been that they contain a single processor in which virtually all user directed computations are performed. The processor is connected to some quantity of memory and other storage devices. The users may submit work to the processor via jobs or through interactive commands. The input/output devices typically have limited, if any, computing capability. Examples of these systems include the ubiquitous personal computer, Digital Equipment Corporation VAX computers, and the CRAY computers.

Advances in computer technology are beginning to erode this 'traditional' view of computer systems. Workstations operating as terminals to centralized systems pose an interesting challenge for the user, computer security officer, and computer security policy. However, the use of workstations or multiprocessor systems does not alter the policy perspective of a centralized computer system accessed by multiple users operating from remote terminal devices.

### 3.2. Distributed Computer Systems

Distributed computer systems are characterized by the distributed or decentralized processing of information. Distributed systems must be based on the capability of transferring the necessary information among the cooperating processors. Typically, the communication resources are provided by a computer network.

Distributed computer systems can be separated into three broad categories. The categories are true distributed systems, systems with distributed functionality, and distributed computing resources or extended computer networks.

#### 3.2.1 True Distributed Computer Systems.

True distributed computer systems are based on a set of autonomous computers communicating via a network. The distributed systems are designed to give the user the perspective of a single, integrated computing facility. The integrated facility is supported even though the services are provided by a variety of computers, possibly in different geographic locations. True distributed systems are characterized by transparency, concealment of separation, and complete trust among the cooperating components.

Distributed systems present the computing resources to the user in a completely transparent manner. This transparency allows the user to depend upon the system to maintain the availability of resources.

The cooperating resources must completely depend upon the correct functioning of the security mechanisms present in the other nodes. The security mechanisms are distributed among the resources and rely on secure communications channels to exchange security information. Security of these systems can only be evaluated by considering the entire system as a single entity.

**3.2.2. Distributed Functionality.** Another view of distributed systems is one of distributed functionality. These systems are characterized by the assignment of specific functions (e.g., file server) to different nodes in the system. These systems are also characterized by a high degree of trust between the cooperating components. Some examples of these systems are the commercially available local area networks and the larger computer networks at the many DOE facilities.

Each of the nodes must rely on the correct functioning of the security mechanisms (e.g., file access controls) in other nodes. Security in these systems can be evaluated only by considering the security functions contributed by all nodes in the system.

**3.2.3. Distributed Cooperating Resources/ Computer Networks.** A more ubiquitous form of distributed system in DOE is the distributed cooperating resources or extended computer networks. These systems are characterized by heterogeneous, independent computer systems that communicate via messages. Examples of these systems are networks with computing systems that collect information from computer-based peripheral devices (e.g., instrument controllers).

## 4. DOE COMPUTER SECURITY POLICY

The DOE computer security policy for all computer systems that process, store, transfer, or provide access to classified information is described in DOE Order 5637.1, "Classified Computer Security Program." [2]

### 4.1. Current Perspective

The DOE policy is implicitly based on the traditional view of centralized computer systems. The DOE policy assumes that any computer that processes

classified information is subject to the entire spectrum of threats and requirements. The policy also considers that any computer connected to a system that processes classified information is subject to the same threats and requirements. The premise is that any computer may be used to access classified information. The policy briefly acknowledges the issues of access control, remote user identification, and configuration control in basic computer networking without any details.

The policy outlines the computer security requirements necessary to establish a proper environment for processing classified information. These requirements include personnel security, physical security, communications security, hardware and software security, and the appropriate administrative procedures.

The DOE policy views each computer system as a self-contained entity that must implement a complete set of security mechanisms. The policy does not distinguish between the functions or security properties of each node in a network.

The absence of guidance on policy interpretation for computer-based devices and distributed systems requires the security officer to prove the system is adequately secure without any criteria for assessing the security. The result is pressure to require that computer-based devices conform to all requirements in the policy.

### 4.2. Computer-Based Instrument Perspective

The connection of computer-based instruments and controllers to computers processing classified information requires these devices to conform to DOE computer security policy. The computer-based devices raise several important security issues because they may provide access to classified information on other computers. Among the issues are user identification and authentication, audit trails, and information access controls.

If an authorized human may routinely use the instrument computer, then the system must meet the requirements in the DOE policy. If routine human access via the instrument is not allowed, then the software in the instrument may be viewed as the "user." In this case, only limited security mechanisms are needed in the instrument. These mechanisms must include physical controls on human access (e.g., locks and lack of keyboards), access controls on the data and software to prevent unauthorized changes, and software engineering practices.

Regardless of the "user" perspective, the security mechanisms in the instrument must be documented in an ADP security plan. Once the plan has been approved, the instrument must be included in the security test, certification, and accreditation of the network.

### 4.3. Distributed System Perspective

The DOE policy can be interpreted as covering distributed systems if one takes the view that a distributed system can be treated as a single system. This integrated view can support the application of the policy with a minimum of change. The integrated view will minimize the impact on existing computing activities in DOE by considering the security functions contributed by each member of the network.

However, even with the integrated view, the existing policy is still inadequate for distributed systems. The policy must be upgraded to provide guidance on how to distribute the security mechanisms throughout the system or network. Specifically, the policy should explicitly allow the distribution of security controls if

- each active process or user is confined to a single component,
- the process or user can access only information on that component,
- every component enforces the same accountability and access control policies, and
- all communications channels between the components are secure.

The access control policy must include discretionary and mandatory access requirements. The accountability requirements must include user identification, user authentication, and audit of actions on the system.

The DOE policy should be extended to guide the interpretation of the access control and accountability requirements for distributed systems. Additional research is needed to establish how the requirements may be distributed among the components of a distributed system.

## 5. ALTERNATIVE APPROACHES UNTIL POLICY CHANGES

Because the existing DOE computer security policy does not support distributed systems, alternative

approaches are necessary to balance the need for distributed systems and policy requirements.

The most important consideration is the acknowledgement that a distributed system processing classified information must conform to DOE computer security policy. The DOE policy contains the ability for the accrediting authority to approve alternative security mechanisms if the systems cannot meet the requirements or the implementation costs are prohibitive. Discussions between developers and accrediting authorities can result in an effective, alternative approach to meeting the policy requirements.

A reasonable compromise is to view the distributed system as a single system with most of the security controls implemented in the general purpose components. Devices, such as computer based instruments, can contribute to overall system security by using the appropriate security mechanisms. The security mechanisms could include access controls on data and software, integrity checks on running software, physical security, controls on user access to the device, and adoption of software engineering practices that inhibit unauthorized changes.

## 6. SUMMARY

The existing DOE computer security policy must be updated to support the distributed computing environments now in use in DOE facilities. The policy changes must support the distribution of security mechanisms among the system nodes. The policy must also provide guidance on evaluating security in a distributed system. The long lead time to update the policy will require the development of interim guidelines to ensure that existing and near-term systems are adequately secured.

## REFERENCES


1. G. Coulouris and J. Dollimore, *Distributed Systems: Concepts and Design* (Addison-Wesley, 1988).

2. DOE Order 5637.1, "Classified Computer Security Program," January 29, 1988.